AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

THE CYBER WAR:

MAINTAINING AND CONTROLLING THE "KEY CYBER TERRAIN" OF
THE CYBERSPACE DOMAIN

by

Neal Jackson, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of Graduation Requirements

Instructor: Dr. Edward Ouellette

Maxwell Air Force Base, Alabama

June 26, 2016

i

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Acknowledgements

I would like to express my sincere appreciation to my wife, for her hours of editorial support and her encouragement. I appreciate the Air Command and Staff College, On-Line Master's Degree Program, for providing me this opportunity. I truly have learned much about cyber war and key cyber terrain. Thank you to Dr. Ed Ouellette, my academic advisor, for your editorial guidance and support. I especially acknowledge my classmates for their timely feedback, some of which added tremendous credibility to this paper.

Table of Contents

Table of Figures

Abstract

Throughout military history, the combatant who controlled the "high ground" or the key terrain has had the tactical advantage that would deny the adversary any leverage due to geographic position. The definition of critical geographic terrain is clear. It may include a hill, a crossing point of a river or lake, or a valley.[1] Dominance of the topography will likely be the deciding factor in winning a battle.

Just as in the geographic domain, there are vital elements of the cyberspace domain. An understanding of these components or *key cyber terrain* is critical to the success of any military operation.[2] The control of this domain affords the commander an unencumbered ability to communicate, plan and operate in cyberspace. In fact, the Air Force cyber mission for the Joint Force Commander is to retain freedom of maneuverability in cyberspace and to deny it from adversaries.[3]

This study uses the problem/solution strategy to assess options that will enable the commander to realize the Air Force's cyber mission. Recommendations will be made that will enable complete dominance of the cyber landscape. Implementation of these recommendations will lead to successful achievement of military objectives.

Introduction

In today's rapidly changing and technologically advanced battlefields, each engagement demands a distinct analysis from any other. In order to adequately gain dominance, the Joint Force Commander (JFC) must comprehend all terrain vital to the operation, including that of cyber. Processes to analyze, map, defend, and control unique geographic features have been well proven and documented. However, there is no Standard Operating Procedure (SOP) at the JFC level to help the commander in the pursuit of cyberspace dominance.

Successful military operations require a detailed analysis of the situation. In military guidance this is referred to as the Intelligence Preparation of the Operational Environment (IPOE).[4] Along with identifying enemy positions and capabilities, an essential part of IPOE is to create a thorough study of critical geographic terrain.[5] The U.S. Army describes this *key terrain* as "any locality or area, the seizure or retention of which affords a marked advantage to either combatant."[6] Once this vital ground is identified, military planners can focus their efforts on positions that will give them both offensive and defensive advantages.

Another aspect of IPOE is the analysis of the "information environment," which is the "environment where humans observe, orient, decide, and act (commonly referred to as OODA Loop) upon information, and is therefore the principal environment of decision making."[7] The "Cyberspace Domain," a significant part of this environment, consists of networks and infrastructures linked together and used to store, exchange, and modify important information.[8] Military communication, relay of commands, vital weapon systems, and cyber related equipment all function within this domain.

Significance of the Study

The term "key cyber terrain," a relatively new term, is not well identified or understood. Current literature refers to this terrain as those elements in the layers of the cyberspace domain that if attacked, can result in damage or even failure of cyber systems vital to the JFC's operation. Nevertheless, there is some disagreement as to what the components of this terrain may include and how it should be assessed and mapped. Most researchers have agreed that recognizing critical terrain will enable the accomplishment of the JFC's cyber mission. However, there is very little information and no official guidance to help the JFC recognize the crucial cyber terrain of a given operation.[9] This paper will present a solution to assist the JFC in achieving cyberspace dominance.

Background

In the modern world of advanced technology, control of cyberspace can be more critical than the control of the geographic landscape.[10] Today's weapons can accurately be deployed remotely and from long distances without an actual presence on the battlefield. To gain the advantage that the control of cyberspace offers, the JFC must have the same level of understanding of cyber terrain as geographic terrain. This comprehension can only come from a thorough analysis of the cyberspace domain. Although there are some similarities to the geographic landscape, there are significant differences as well.[11] These differences are not necessarily intuitive. For example, some believe that cyber terrain is only comprised of components that are tied to the physical and geographic planes, such as routers, switches, and other devices. However, critical cyber terrain as suggested by Fanelli[12] is also comprised of logical, cyber persona, and supervisory planes that are not attached to any one location. The

following is a description of these five planes as defined by Raymond,[13] and will serve as a definition of key cyber terrain. The five planes are also illustrated in Figure 1.[14]

1) Supervisory Plane. The supervisory plane provides the oversight and the authority to start, stop, modify, or redirect a cyber operation. Cyber terrain at the supervisory plane is comprised of elements of cyberspace that either perform a supervisory function or provide a conduit for command and control.

2) Cyber Persona Plane. The cyber persona plane identifies identities in the cyber domain. These identities might have a many-to-one or one-to-many relationship with physical individuals. Here cyber terrain includes such features as user accounts or credentials that provide access to information resources.

3) Logical Plane. This plane consists of the operating system, application software, software settings on a device, and the logical links between networked devices. Terrain at this level includes a wide range of software systems, services, and protocols that keep networks running and computers doing useful work.

4) Physical Plane. The physical plane includes components of a computer system and attached hardware. This plane is comprised of the devices that are often interpreted as being cyber terrain, such as the routers, switches, and other network devices that physically connect components in a network.

5) Geographic Plane. The geographic plane is the physical location where the information system or parts of the system reside. It is the most static of all the planes. While the logical cyber location of a system is usually more important than the geographic location of a network component, failure to recognize the importance of the geographic plane can be costly.
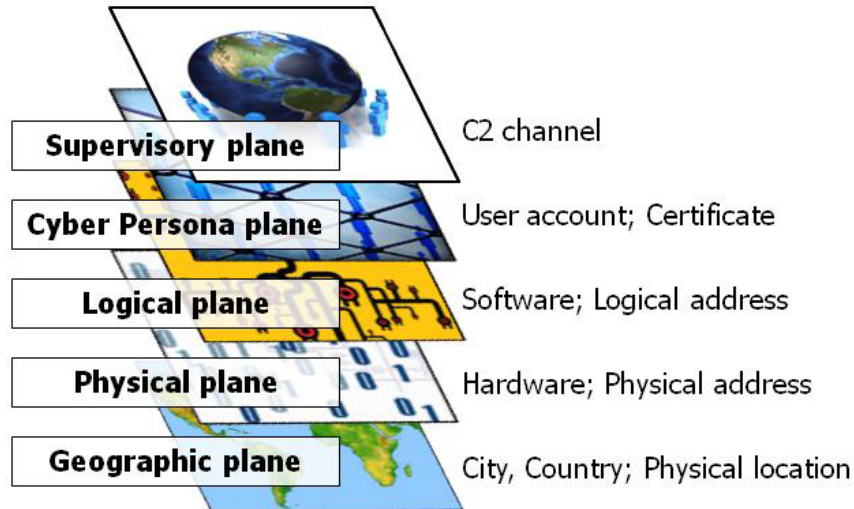
Figure 1. Cyberspace Planes with Representative Examples [15]

The Vulnerability of Key Cyber Terrain

Understanding and recognizing key cyber terrain, though critical, does not provide everything the JFC needs to preserve and protect military cyber power. The joint force must have the ability to quickly and efficiently respond to cyber-attacks. It must also plan and execute strikes against the enemy's persona, logical, and physical planes of key cyber terrain. These planes are the most accessible, vital and vulnerable elements in cyberspace. For that reason they make up the surface that adversaries would likely attack in order to disable the cyber capability of the joint force (see figure 2). The geographic and supervisory planes are not included in the attack surface because they are not as easily accessible and are well defended.[16]
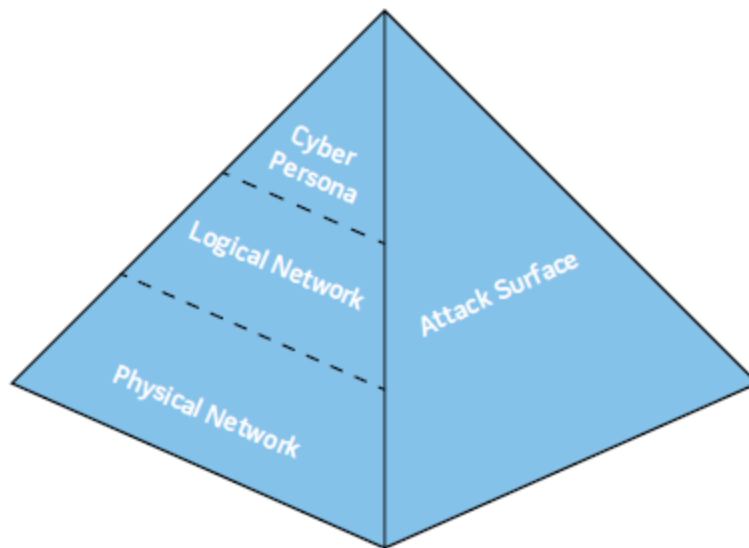
Figure 2. Cyberspace Attack Surface[17]

Commanders have vast practical experience and knowledge in deploying forces to protect and attack geographic and physical targets. However, the education and experience needed to formulate defensive and offensive plans for the vulnerabilities of cyber terrain is currently lacking at the senior leadership level.[18] To compound the problem, current documentation does not provide the guidance that the JFC requires for planners and strategists to plan and generate an attack or a defense of cyberspace.[19] To help fill the gap, in 2015, the Department of Defense (DoD) released a new strategic document called the *Department of Defense Cyber Strategy*. This strategy defines five strategic goals to defend the United States from cyber-attack and to "build and maintain ready forces and capabilities to conduct cyberspace operations."[20] This high-level document clarifies the goals and organization of the US Cyber Command (USCYBERCOM) in support of the joint forces. Nevertheless, there are still no SOPs at the JFC level to guide the commander. To be successful, the JFC must have direction as to how to proceed in tactical cyber situations.

Dominance in cyberspace is crucial to every aspect of the modern battlefield. Its unencumbered access is vital to communications, operating and firing modern weaponry, conducting intelligence, surveillance, and reconnaissance (ISR), assessing an opponent's position and intentions, as well as providing indications and warnings of planned adversarial attacks. The loss of any of the cyber terrain planes would be a severe blow to the JFC's objective. The commander's ability to create and execute detailed plans would be dangerously restricted.[21]

Mapping Key Cyber Terrain

A map of cyber terrain is a representation of the knowledge and/or assumptions of the five terrain planes that determine or influence cyber decisions.[22] Mapping is the process of collecting evidence of real or assumed cyberspace elements and determining their validity. Deborah Bodeau, in *Mapping the Cyber Terrain,* contends that a map will help determine whether:

- Assumptions about features of the cyber terrain (e.g., adversary characteristics and possible adversary actions) are consistent.
- A claim or hypothesis is meaningful to a specific real-world situation or can be evaluated in a given environment.
- A set of claims or hypotheses assume the same environment and thus could be evaluated in a common integration experiment.
- Evidence or analytic results obtained in a given evaluation environment could be used to confirm or disconfirm a given claim or hypothesis.
- A claim or hypothesis supported by evidence from a given evaluation environment could be – or could fail to be – meaningful and relevant to a given real-world situation.[23]

The framework used to build a map and test its validity includes the construction of three environments.

1) *The Claims Environment* contains descriptions of assumptions, claims, and hypotheses about the five planes of the adversary's key cyber terrain.

2) *The Real World Environment* is where evidence is sought to prove or disprove assumed claims.

3) *The Evaluation Environment* applies derived evaluations to verify or dispute claims.[24]

These three environments need to be coordinated. For the hypotheses or claims to be meaningful, the claims environment must match the real world environment or some portion of it. To confirm the validity of claims, the evaluation environment must be constructed with evaluations that match the claims and hypotheses of the claims environment. The evidence obtained during the analysis must represent a part of the real world.[25] Figure 3 represents these relationships.
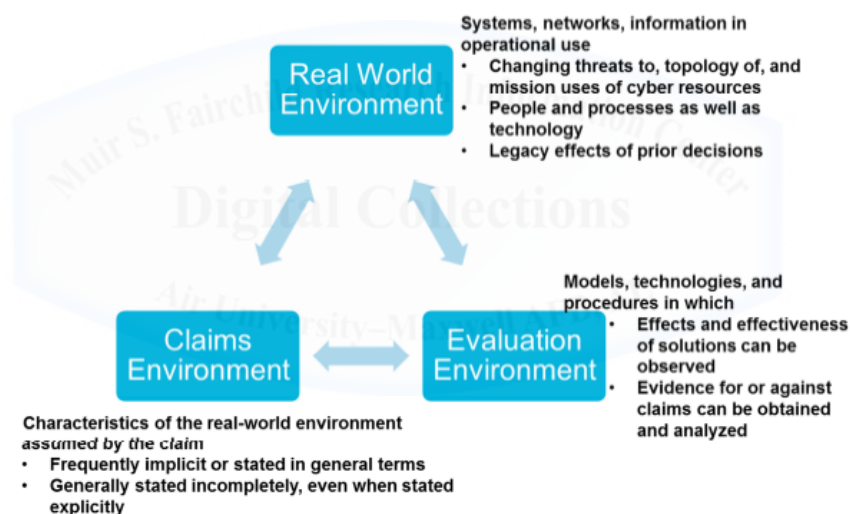
Figure 3. Environments to be Aligned [26]

The construction of the claims and real world environments are straightforward. Their structure is made up of data from the known cyber history of the adversary, recent ISR reports, and educated assumptions based on current cyber activity. Building the evaluation environment is more challenging. There are a wide variety of experiments and tests that can be used to evaluate the validity of the existence and vulnerability of elements in the planes of the cyber

terrain. These range from the simple to the very sophisticated. Most of the cyber evaluations used today draw upon a large body of successful experience in detecting the virtual landscape.[27]

After the elements of the key cyber terrain planes have been identified and verified, the next step in mapping is to develop a model. There are many effective methodologies to model cyber terrain. Some draw analogies with the physical terrain. For example, John Mills, in his article "The Key Terrain of Cyber" states that cyber "has a number of earthly manifestations including data centers, internet service providers, undersea cables, international standards bodies, BIOS [Basic Input Output System], supply chain, the cyber workforce, and the engine of technology innovation."[28] Others, such as Jared Holspopple in Figure 4 of his article "FuSIA: Future Situation and Impact Awareness," use a graph with nodes, networks, and interconnections.[29] Still others use missions and mission dependency to determine which terrain is key, as in Daniel Fava's article, "Terrain and Behavior Modeling for Projecting Multistage Cyber Attacks" and G. Jakobson's article, "Extending Situation Modeling with Inference of Plausible Future Cyber 35 Situations."[30, 31] All of these methods use somewhat complex software and modeling techniques.[32] This process is critical in order to accurately visualize key cyber terrain. An image of the vital elements of cyberspace is necessary for the JFC to defend and attack the operation's virtual landscape.

The problem for the JFC, as stated earlier, is the commander's lack of education and experience dealing with cyber issues. Cyber mapping, especially evaluation and modeling, requires well-trained cyber professionals who understand technology issues and know how to use software or other techniques to model the terrain.

Currently the JFC depends on resources outside of his/her organization for cyber support. For example, the new Department of Defense Cyber Strategy provides support to the JFC through the USCYBERCOM's[33] new task force called "Cyber Mission Force" (CMF). The

CMF has the responsibility to protect the Department of Defense's cyber assets and provide expert support for tactical operations.[34] When the CMF's organization is complete, it will provide more than 6,200 support personnel trained to carry out the USCYBERCOM's missions, one of which is to provide cyber support to the JFC.

Although support forces like the CMF will improve the resources available to the JFC, there still is a lack of Standard Operating Procedures for tactical operations. This can be problematic when dealing with real-time issues. In the absence of cyber savvy staff personnel, communication to the CMF and others in a support position will be difficult. Without documented guidance and SOPs, the commander's staff could become confused when quick cyber-related decisions need to be made. The JFC needs skilled personnel and SOPs to obtain timely professional cyber assistance to fully realize the joint force cyber mission.

Measurement Criteria

Three options will be presented to solve the problem the JFC faces in achieving the joint force's cyber mission. The essential factors that will differentiate the solutions are: 1) timely identification of key cyber terrain, 2) accurate mapping of the cyber terrain, 3) defense of key cyber terrain, and 4) attack of key cyber terrain. The criteria that will measure these options are further defined in the following paragraphs.

Identification of Key Cyber Terrain

The identification of the unique layers of the cyber terrain is the first step in analyzing and understanding the operational cyberspace domain. Before defensive or offensive cyber operations can begin, the elements of the terrain layers must be recognized. Each option will be assessed and compared by its method(s) of accurately and efficiently distinguishing key cyber terrain. The significant points that will be examined are: 1) the ability to establish a process for a

clear and timely identification of the elements in the layers of the cyber landscape, 2) the ability to provide the JFC real-time accurate information concerning the layers of the cyber terrain, and 3) the ability to advise the commander as to which cyber elements are vital to mission success.

Mapping the Key Cyber Terrain

The skill of mapping the terrain of cyberspace will enable the JFC to control the cyber domain. It will reveal important cyber assets and networks and identify where vulnerabilities can be exploited. Unmapped terrain is a limiting factor in the success of modern military operations. For this reason, the ability to map cyber terrain and identify the unique elements of any operation will be used as a criterion to select which alterative best solves the problem of dominating operational cyberspace. Each option will be evaluated as to how the layers of cyberspace domain are mapped and presented to the JCF. The mapping process will be assessed by its efficiency to identify weaknesses of both friendly and adversarial key elements of each terrain layer. Each solution will be appraised for its ability to provide the JFC with accurate information gleaned from the mapping process. An assessment will be made for the capacity of each option to provide expert personnel who understand the software and modeling techniques of cyber terrain mapping.

Defense of Key Cyber Terrain

The defense of cyber assets is vital to maintaining the ability to conduct military operations. The JFC commander depends on these resources not only for communication but also for almost every aspect of the joint force operation. Each of the three option's impact to the defense of key cyber terrain will be measured by its ability to defend and hold vital elements of the five layers of cyber terrain. The defensive strength of each solution will be evaluated by its ability to independently protect the virtual landscape from hostile attacks. Also, an assessment

will be made of its ability to access outside resources, such as the US Cyber Command,[35] for assistance with real-time cyber security issues. Further evaluation will be based on whether the JFC will have total command of the defensive efforts in cyberspace.

Attack of Key Cyber Terrain

The ability to attack and destroy the adversary's cyber terrain is crucial to gaining and maintaining control of the virtual domain. It will effectively divest the enemy from any freedom of mobility in cyberspace and render their systems useless. In today's modern battles, this is analogous to gaining the ultimate geographic high ground.[36] The options will be evaluated on their ability to independently plan and successfully execute attacks on adversarial cyber terrain. As with the defense of the terrain, the offensive strength of the solutions will also be evaluated by their ability to access outside resources in real-time to resolve difficult offensive cyber issues. The JFC's ability to maintain offensive command and control will also be evaluated.

Option Evaluation

The three different solution options are 1) incorporate Standard Operating Procedures, 2) add a cyber professional to the divisions of the Joint Operations Center, and 3) additional training. Each alternative will be described in detail. An analysis will then appraise the options against the four criteria. This evaluation will ultimately serve as a basis for recommending a solution to enable the JFC to dominate the operational cyberspace domain.

Option 1: Incorporate Standard Operating Procedures

Although there now exists a higher level Cyber Strategy, there still is no SOPs for cyberspace tactical operations in current documentation.[37, 38] This option incorporates SOPs into existing policy. It expands the definition of cyber terrain, provides instruction for cyberspace

mapping, and instructs the JFC in how to obtain support for the operation's cyber warfare. Without SOPs, the JFC is at risk of failing to understand how to access real-time support. Using the new Cyber Strategy exclusively, the commander may become confused as to how resources outside the joint force command will help achieve the operation's cyber mission.

Cyber technology is advancing at a speed that is difficult for the cyber novice to comprehend. In many cases military policy makers have little training or experience in the virtual domain. For this reason, cyber professionals, who are at the leading-edge of cyber change, will be assigned to a team developing new guidance and standard procedures for tactical cyber operations. Their responsibility will be to develop processes to recognize and map vital elements in the cyber domain. Along with identifying and mapping critical cyber elements, it is important to know how to defend and attack them. Because of this, seasoned JFCs or other military professionals experienced in planning and executing military campaigns will also be assigned to the team.

Cyberspace is defined in higher level publications as the 'physical network, logical network, and cyber-persona layers'.[39] In current literature, these layers are part of the cyber landscape.[40] The new SOPs will redefine them as cyber terrain planes and expand it to include the supervisory and geographic planes. A detailed explanation of the five planes will be incorporated and guidance will be given concerning the identification of virtual terrain. The new instruction will also explain the importance of cyberspace supremacy on the battlefield and how to obtain and maintain it.

The new procedures will explain the importance of cyberspace mapping and its methodology.[41] It will emphasize that cyber mapping can be complex and that support through the USCYBERCOM's Cyber Mission Force, or other cyber competent personnel, will be

required to strengthen the JFC staff's mapping duties. Also, to ensure currency and competence, the SOPs will require USCYBERCOM to certify that cyber mapping professionals have adequate training and experience.

The new SOPs will describe in detail the assistance available to the JFC and the component commanders for planning and executing cyber warfare. The necessary command and control for cyber support will be explained so that the commander understands how to contact USCYBERCOM and CMF for expert cyber reinforcement. After the team has satisfactorily developed the SOPs and clarified the command and control, it will ensure that they are incorporated into guidance with the necessary documental changes and updates.

Analysis of Option 1

Identification of Key Cyber Terrain

Using cyber experts to describe cyber terrain and document how to identify it will add credibility to the new SOPs. These experts, along with the JFCs on the team, will ensure that the new SOPs are accurate and can be understood by the joint force. This will mitigate the risk of key cyber terrain going undetected.

These new procedures will provide the JFC the tools needed to visualize the complete cyberspace domain and identify vulnerabilities. Cyber warfare planning will be more reliable with SOPs for recognizing cyber terrain.

Mapping the Key Cyber Terrain

The cyber professionals creating the SOPs will understand that cyber mapping is complicated. It is so complex that specialized education and training are required to ensure that

the cyber map is correct. Using experienced JFC's on the team will make certain that the guidance explicitly directs the joint force to use the CMF of the USCYBERCOM.

The new instruction to seek expert assistance to complete the task of mapping cyber terrain gives credibility to the process. It will decrease the risk of misidentifying the virtual landscape planes. Also, following this instruction will increase the ability of the force to gain control of the cyberspace domain.

Defense of Key Cyber Terrain

Cyber defensive instructions developed by a team of cyber professionals and seasoned JFCs will be indispensable to the commander as he/she struggles to successfully conduct cyber warfare. If the JFC follows the new procedure and accesses available cyber assistance, the likelihood of victory will increase exponentially. It may very well determine the success of the mission.

The guidance on the maintenance of C2 communication links will arm the commander with the means to access the all-important CMF for expert assistance in cyber warfare. With these command communication lines open, help can be readily available as the situation changes.

Attack of Key Cyber Terrain

Just as with defense, if the JFC observes the new SOP, the chances of attacking cyber assets and winning the cyber war increases dramatically. Cyber professionals who are part of the team developing offensive procedures understand the cyber terrain and its vulnerabilities. For this reason, the instructions for the cyberspace assault will explain attack surfaces and provide viable paths for success. Winning the cyber war is dependent on reliable well-defined processes and guidance. This option fulfils this need that has been absent in current documentation.

Option 1 Strengths

The new SOPs for cyberspace operations fill the gaps in existing guidance with a clear definition of key cyber terrain and cyber war guidance. Their explanation of cyber terrain mapping and its importance to cyber terrain dominance will add to the joint force's ability to understand the cyber elements that exist in the operation and which ones should be defended and exploited. The new SOPs will instruct the JFC to use existing expert cyber organizations (i.e. the Cyber Mission Force) for cyber mapping and assistance in planning offensive and defensive maneuvers. This support will help fill the void of expert cyber professionals in the joint force organization.

Option 1 Weaknesses

This alternative does little to provide the commander with competent real-time cyber expertise within the joint force. Expending the time needed to contact the CMF for mapping and planning assistance will place the opportunity for seizing and defending virtual terrain at risk. Also, relying on an organization outside the control of the JFC can lead to miscommunication and planning mistakes. With rapidly changing cyber technology, a specific and detailed SOP that defines the planes of cyber terrain and includes specialized guidance is at high risk of becoming obsolete soon after it is finalized and approved. History has shown that skills are not acquired by just studying guidance; experience is also needed. Also, this option does not provide for training of the JFCs. This creates a risk that the SOPs will be misunderstood and grave mistakes could be made.

Option 2: Add Cyber Professionals to the Divisions of the Joint Operations Center

High level publications place accountability of cyberspace operations with the JFC. But there is no provision for the commander to retain expert cyber professionals within the joint force command.[42] The new DoD Cyber Strategy[43] places responsibility for strategic cyber

control and tactical support with the USCYBERCOM and the CMF, but there is nothing to help

the JFC plan tactical operations to gain cyber supremacy. In order for the JFC to dominate the

virtual domain, the commander must have skilled personnel within the joint force organization.

These cyber experts will enable the joint force to recognize key cyber terrain, map it, and

develop executable plans to defend and control it. These skilled professionals must have a clear

means to quickly access the support of USCYBERCOM when cyberspace is more complicated

and complex than they can manage.

The Joint Air Operations Center (JAOC), "provides operational-level command and

control (C2) of air component forces as the focal point for planning, executing, and assessing air

component operations."[44] This center supports the JFC in all of the joint force air objectives. It

is also accountable to create and evaluate viable Courses of Action (COAs). After the

evaluation, the center recommends to the commander the COA that has the best chance of

achieving the mission's objectives to the commander.

The JAOC is divided into five divisions: strategy, combat plans, combat operations, ISR,

and air mobility.[45] These highly specialized teams depend on cyber systems to achieve their

assigned responsibilities. The failure of these systems will result in grave consequences and

must be protected. Moreover, because of its ability to assess the enemy's capabilities, the JAOC

is in a unique position to recognize and attack the elements of the adversary's systems. In most

cases, the JAOC lacks the expertise to understand the cyberspace domain and its variabilities.

This option proposes to assign highly trained CMF professionals or other qualified cyber

experts to each of the divisions of the JAOC. These cyber specialists will become part of the

JAOC and have the responsibility to recognize and map the cyber landscape. They will advise

the JAOC in the creation of plans to defend friendly terrain, and gain control of the adversary's

terrain. They will also be responsible for communication and support from USCYBERCOM's

Cyber Mission Force.

In order to avoid miscommunication, these experts will have authority to discuss cyber

defensive and offensive plans with the commander. Figure 4 illustrates the addition of cyber

professionals to the JAOC organization. The dotted line represents a direct line of
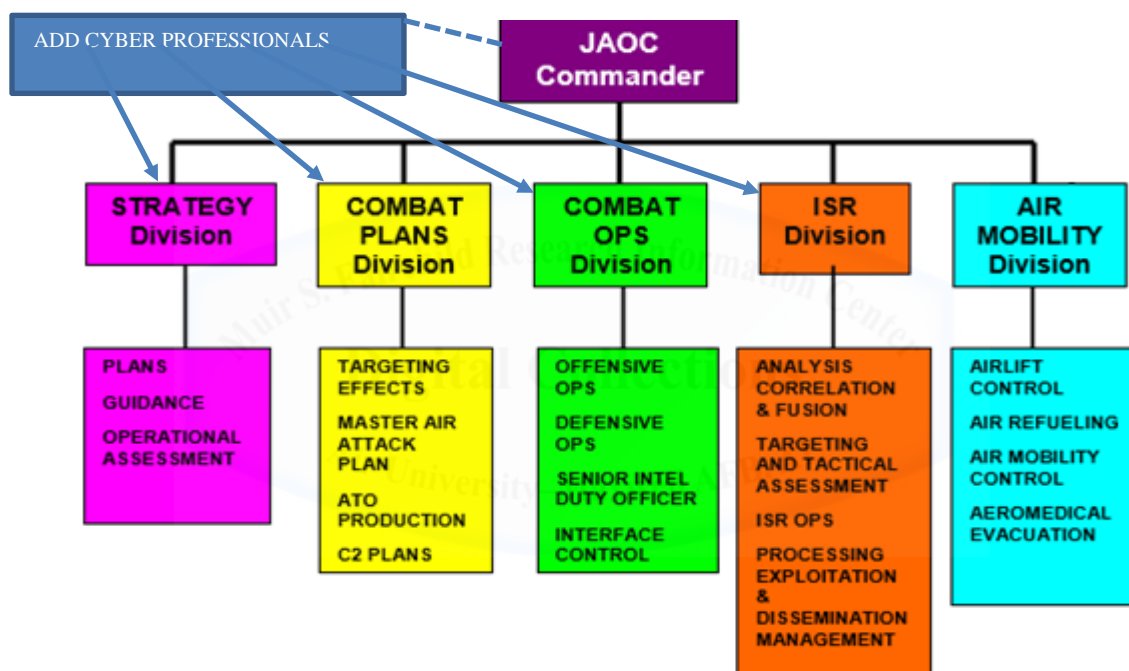
communication to the commander.

Figure 4. Addition of Cyber Professionals to the JAOC[46]

Analysis of Option 2

Identification of Key Cyber Terrain

The cyber experts will have the training and experience to identify the five planes of the

unique virtual terrain. They will be intimately familiar with the elements that make up the planes

of cyberspace and understand how to recognize weaknesses in the landscape. Having these experts on the JAOC's team will provide cyber terrain knowledge that has been sorely missed.

Identification of critical elements in cyberspace is the first step in cyber war planning. This option will improve the JAOC's ability to recognize key cyber terrain and increase its ability to produce usable plans that will lead to success. This option will give the JAOC an excellent grasp of the critical virtual terrain and provide a basis for gaining control of it.

Mapping the Key Cyber Terrain

Since the cyber professionals will have current training in cyber terrain mapping, they will provide an unparalleled ability to develop an accurate real-time map of the cyber landscape. Because they are certified cyberspace mappers, they provide a unique ability in cyber terrain mapping to the joint force. Their experience and training will provide confidence that cyber maps will be accurate and contain all of the existing elements of the five cyber terrain planes. These experts will be vital to the joint force in identifying the components of cyberspace through the mapping process. Once these maps are generated, the joint force can confidently plan virtual defense and attacks.

Some cyber maps may be extremely complicated. The cyber professionals in the JAOC will provide the expertise to interpret complicated cyber maps and other documents. With the incorporation of professionals, the risk of mistakes caused by unmapped cyber terrain is greatly reduced.

Defense of Key Cyber Terrain

Armed with a viable understanding and map of the five planes in the virtual terrain, the JAOC is well equipped to defend the cyberspace domain. With cyber professionals on the staff

of the JAOC, defensive planning and execution can be monitored and adjusted real-time as the situation changes. The JFC will have confidence that the joint force's critical cyber components will be defended from enemy attacks.

With the inclusion of the cyber experts, the JAOC will become more sensitive to defending critical cyber assets. Joint Air Operations Center planners will be more likely to consider defending cyber terrain when creating and evaluating Courses of Action for the JFCs approval. As the joint force becomes more cyber responsive, the commander will also be more likely to consider cyber in his/her decisions and actions.

Attack of Key Cyber Terrain

As with defense, the attack of the enemy's cyber domain will have the best chance of being successful with knowledgeable cyber professionals at every level of the JAOC team. Most of the risks associated with attacking the elements of adversarial terrain will have been eliminated or at least mitigated.

The new cyber sensitivity brought to the JAOC will also improve attack planning. The cyber professional will assist the JAOC planners in understanding the cyber-attack surfaces and in planning cyber warfare. With the inclusion of these experts in the JAOC, the JFC's advantage gained from disabling the adversary's cyber system increases greatly.

Option 2 Strengths

Adding cyber skill and experience to the JAOC gives the JFC an excellent opportunity for cyberspace superiority. CMF personnel trained by USCYBERCOM, assigned and reporting to the joint force leadership, will be vital to operational success. With the communication lines open to other experts, these new members of the JAOC will have unmatched resources to

identify, map, defend, and attack the cyber landscape. The response to changing situations during the operation can be dealt with in real-time with team members experienced and trained in cyber warfare.

Option 2 Weaknesses

With this option, there is no evidence that guidance will change. There is no direction to instruct the JFC to configure the JAOC with a USCYBERCOM trained professional in every division. This lack of configuration control can lead to unacceptable variations in joint force organizations. There is a risk that if there is no written SOP to include cyber experts in the JAOC divisions, they will not be included in the organization. Also, there is no guidance to verify that the cyber professionals have the expertise and training required for identifying, mapping, and planning defensive and offensive cyber maneuvers. Additionally, there is no allowance for training the JFC in how to include the cyber professionals into the joint force organization. Without training and written guidance, there is a risk that the cyber experts will be assigned to tasks not related to cyber.

Option 3: Additional Training

This option advocates additional training for the JFC and staff. Additional instruction is needed because current guidance is deficient and does not provide the JFC all the direction needed to successfully identify vital cyber terrain, map it, and plan offensive and defensive maneuvers. The new Department of Defense Cyber Strategy provides strategic high-level instruction but does not offer any tactical direction. Because of this, the joint force may be vulnerable to cyberspace attacks and struggle offensively. Also, since there is an assumed lack of cyber experience and education at the JFC level, the commander will need instruction in how to coordinate with the liaison of the Cyber Command when planning cyber warfare.

To fill the holes in current documentation, training will first expand the definition of cyber terrain found in current guidance to include all five of its layers.[47] The joint force will then be taught to recognize the elements of these planes and learn how to defend and exploit them.

Once the planes are identified, a map of the cyber terrain will reveal where the attack surface is most exposed. Cyber mapping is complex and its methodology is constantly changing. The joint force will not have the time or the education to produce accurate cyber maps that will be useful for offensive and defensive planning. For this reason, instruction will be given to help the Commander and staff to access cyber experts, such as USCYBERCOM and the CMF, for cyber mapping support.[48]

Command and Control (C2) in the cyber domain is constantly evolving. Trying to keep pace with advances in technology is challenging. It is difficult for the Commander to maintain currency in cyber C2, given all his/her other responsibilities. To offset this difficulty, Commanders and their staff are to be trained in maintaining clear lines of communication with USCYBERCOM. This ability to clearly communicate requests for support and to receive needed assistance, will allow the Commander to properly utilize supporting resources. This will allow the JFC to stay focused on achieving each mission mission objective.

Clear standard procedures for cyber warfare tactics are not found in current guidance. To mitigate this, new training will be developed to prepare the joint force to defend and attack the cyber terrain planes. To be of value to the JFC, the training will: 1) explain the attack surface of the cyber planes (see figure 2) and its vulnerabilities; 2) define resources available for cyber mapping and related issues; 3) explain the importance of cyber C2 and how to use it to access cyber support; 4) clarify current methodology for cyber warfare; 5) emphasize the joint force's vital responsibility to dominate the cyberspace domain; 6) stress that gaining control of cyber

terrain is as important as or more important than attainment of the high ground in the traditional battles;[49] and 7) make clear that the force that controls key cyber terrain will have the decided advantage in the conflict.

Analysis of Option 3

Identification of Key Cyber Terrain

Training the JFC and his staff in identifying cyber terrain will provide them the tools needed to recognize vital cyber components. If the training is conducted well, the risk that cyber terrain will be unidentified will be reduced. With this instruction, the JCF will have increased confidence that all critical cyber terrain, both friendly and adversarial, will be revealed. This assurance will increase the JCF's confidence that the cyber warfare planning will consider all the five planes of the unique cyberspace of his/her mission. This will increase the probability that the commander will be successful in obtaining the mission's cyber priorities.

Mapping the Key Cyber Terrain

The training will outline mapping techniques and methodology, but because of cyber terrain mapping complexity, emphasis will be placed more on how to gain assistance from cyber mapping professionals. Giving mapping responsibility to educated and experienced specialists will avoid overstretching the joint force, jeopardizing its ability to focus on mission objectives. The training will also simplify the process of accessing cyber experts. The instruction of the JFC and his staff will enable them to comprehend the C2 of the USCYBERCOM and how to request cyber mapping support. Because of the ever-evolving C2 of this cyber support, it will be stressed that open communication lines with USCYBERCOM must be maintained to gain timely cyber mapping assistance.

Defense of Key Cyber Terrain

The training received to identify and map cyber terrain will increase the ability of the JAOC to plan cyber defense. Also, as the planners and strategists learn to access professional cyber assistance their credibility will increase. The operations center's confidence that cyber war planning will result in cyberspace dominance will expand with this instruction. Since the training will sensitize the JAOC to cyber control, the development of the Courses of Action presented to the JFC will include cyber terrain defense.

Attack of Key Cyber Terrain

Successful offensive tactics are dependent upon a cyber savvy force. This new training will provide the skills to plan an attack on the adversary's virtual terrain. The new cyber sensitivity will insure that cyber-attack planning is also included in the Courses of Actions presented to the JFC. This new training increases the ability of the joint force to successfully attack the adversary's cyber terrain and gain control of the operation's cyberspace.

Option 3 Strengths

Because of the absence of tactical cyber SOPs, this training will fill the documentation gap and instruct the JFC and staff in how to obtain the tools needed to grasp control of their mission's cyberspace domain. It will provide the skills needed to recognize cyber weakness and strengths and how to map and exploit them. The new instruction will teach the JFC and staff how to access and use the USCYBERCOM expert assistance when faced with the complexities of cyber mapping and war planning. This training helps to mitigate the risk of losing tactical opportunities because of mistakes caused by cyber ignorance and inexperience.

Option 3 Weaknesses

The obvious weakness is that before staff members can be effective, they must be trained in cyber awareness and warfare. With staff turnover, the joint force effectiveness will be inhibited by any untrained staff member's inability to respond quickly and decisively to cyber issues. Another weakness is that with the speed that cyber technology changes, training will rapidly become outdated. The joint force will constantly be in need of updated instruction. Also, there is a risk that the added required training will divert the joint force from focusing on the mission objectives.

Comparison of Options

An option comparison chart will be used to rate how well each option fairs against the evaluation criteria. An explanation of assessment rationale for each alternative will follow.

Option Comparison

Evaluation Criteria	Option 1	Option 2	Option 3
Identification of Key Cyber Terrain	+	0	0
Mapping the Key Cyber Terrain	0	+	+
Defense of Key Cyber Terrain	-	+	0
Attack of Key Cyber Terrain	-	+	0

Key:
+ Superior
0 Average
-   Poor

Figure 5. Option Comparison Chart[50]

Comparison Rationale

Option 1

Option 1 was rated superior for Identification of Key Cyber Terrain because adding SOPs to current guidance has an excellent chance of providing the JFC with clear and simple instructions in identifying critical cyber terrain. Although cyber technology is rapidly evolving, the methods of identifying elements of vital terrain remain fairly stable. The elements may become more complicated and have more advanced capability, but the techniques for detecting them will most likely remain relatively constant. For his reason, adding sound procedures and current guidance will enable the JCF to accurately recognize cyber terrain.

Mapping cyber terrain is a new concept. Mapping methods are currently evolving as new technology is developed. Adding instruction to current documentation is at risk of rapidly becoming out dated. Still, the current mapping methodology is well thought-out and if the JAOC is even somewhat cyber savvy, with clear written instruction, it has at least an average chance of successfully mapping the key terrain of cyberspace. This is the reason that option 1 was given an average rating for mapping the key cyber terrain.

Knowing how to defend any important terrain requires more than just written instructions and standard procedures. Well prepared cyber warriors also require training and experience. These have always been essential elements in developing defensive skills in the domains of warfare. It is no different for cyberspace. Because of this, option 1 was rated poor for defending key cyber terrain. Option 1 was rated poor for attack of key cyber terrain for the same reasons as it was rated poor for its defense. Warfighters need cyber experience and training, not just SOPs.

Option 2

Identifying the elements of cyberspace does not necessarily require specialized training or experience as long as the recognition method is properly documented. The joint force staff usually has enough skills that with SOPs it can successfully recognize key cyber terrain. Option 2 was rated average for cyber terrain identification since it is true that cyber professionals can recognize the components of cyberspace, but without guidance they may not know which of these elements are key.

Cyber mapping techniques are more an art than science. For this reason documenting how to generate a cyber map is difficult. That is why trained and experienced cyber professionals are essential to create an accurate and useful map of cyber terrain. For this reason option 2 was rated superior for cyber terrain mapping.

Success in warfare is heavily dependent on the experience and training of those fighting the conflict. It is no different in cyber warfare. Because each situation is unique, trained and skilled cyber professionals are exceptionally capable of defending and attacking the rapidly changing cyber landscape. This is why option 2 was rated superior for defending and attacking key cyber terrain.

Option 3

Option 3 was rated average for cyber identification because if training is the only way to learn how to recognize cyber terrain, it has only an average chance to be effective. If procedures are not documented the training will be susceptible to unauthorized changes. The warfighter will be at risk of inadequate training which may result in the reduced ability to identify cyber terrain.

Cyber mapping is heavily dependent on the skill and experience of highly trained cyber professionals. The instructions that are available cannot explain adequately how to map

cyberspace. It is almost impossible to generate a cyber map with just written instructions. The assistance of cyber experts is required. Option 3 will provide the training needed to allow the JFC to successfully access the qualified help needed for cyber terrain mapping. For this reason option 3 was rated superior for key cyber terrain mapping.

To become an effective warfighter, training and experience are required. If either one is left out, there is a higher risk of danger and incompetence. Option 3 was rated average for both defense and attack of key cyber terrain because training alone will not provide the JFC success in cyber warfare.

Recommendations

Based on the comparison chart it would appear that option 2 would be the solution to providing the JFC the tools needed to accomplish the commander's cyber mission. Having USCYBERCOM certified professionals on the JFC's staff is certainly vital to all aspects of cyber warfare. But when the ratings are studied, it becomes obvious that each of the options have superior characteristics. It would be irresponsible not to consider the exceptional qualities of each option as part of the solution. In fact, when examining the options, the weakness of one option is the strength of another. For example, option one provides new SOPs to fill the gaps in present guidance, but it does not provide training or require cyber professionals as part of the JFC's organization. Option 2 offers trained cyber experts but does not solve the guidance and training deficiencies. Option 3 ensures that the JFC's staff has cyber training but there is still no documented guidance or cyber professionals to sustain the training.

Therefore, there are three recommendations to ensure that the JFC can achieve the joint force cyber mission:

1) Revise the JAOC organization to include USCYBERCOM certified professionals to join its strategy, combat plans, combat operations, and ISR divisions.

2) Use cyber professionals, experienced JAOC commanders, and seasoned JFCs as a team to develop SOPs that 1) require USCYBERCOM certified professionals to join the four previously mentioned divisions of the JAOC, 2) add a complete description of key cyber terrain and how to identify the unique cyber elements of an operation, 3) require that the JFC only allow USCYBERCOM certified professionals to map cyber terrain and 4) require periodical cyber training for military personnel as outlined in option three.

3) Design training based on the guidance developed in the second recommendation. This training will be required for all Joint Force Commands and staff. This training can be in the form of training seminars or part of a curriculum needed to be eligible of Joint Force Command or a member of a JAOC.

These recommendations will ensure that the JFCs have a well-trained and experienced cyber savvy staff. The gaps in current guidance will be resolved so that the commanders have written documentation to guide them when they are faced with the unique cyber terrain of any mission.
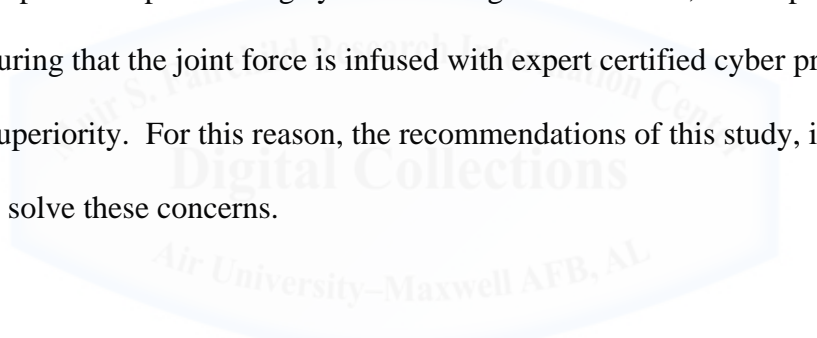
Conclusion

The rapidly changing technology of cyber has left the US DoD in danger of losing tactical advantages that have been gained over the last half century by unprecedented industrial superiority. As the world becomes more controlled by computers and the free flow of virtual

knowledge increases, the risk of enemies winning the cyber war intensifies. There are many examples of adversaries gaining access and corrupting sensitive economic and defensive cyber systems. It is therefore imperative that dominance of the virtual landscape be won and defended with the same vigor as that of the physical landscape.

The cyber landscape is ever changing. It is difficult to stay ahead of cyber transformations. They can happen almost instantaneously. Every effort must be taken to ensure that the joint force has the ability of gaining and holding the 'high ground' of cyberspace.

To win the cyberspace battle, the key cyber terrain must be understood, recognized, and dominated to enable the JFC to achieve the commander's mission objectives. The realization of this conquest is dependent upon solving cyber warfare guidance issues, developing cyber training, and ensuring that the joint force is infused with expert certified cyber professionals to maintain cyber superiority. For this reason, the recommendations of this study, if implemented, provide a path to solve these concerns.

Endnotes

[1] Raymond, David et al, Key Terrain in Cyberspace: Seeking the High Ground. 2014 6th International Conference on Cyber Conflict, NATO CCD COE Publications, 1

[2] Ibid

[3] U.S. Air Force, ANNEX 3-12 *Cyberspace Operations*. 30 November 2011, iv

[4] U.S. Department of Defense *Joint Publication 2-01.3 Joint Intelligence Preparation of the Operational Environment,* 16 June 2009, xi

[5] Raymond, David et al,1

[6] Headquarters, Department of the Army, *Field Manual 3-90-1: Offense and Defense Volume* 1, 2013.

[7] Joint Publication 2-01.3, II-27

[8] Ibid.

[9] Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations," Joint Force Quarterly 61 (2nd Quarter 2011), 11–17

[10] Raymond, David et al, 1

[11] Mills, John R., *The Key Terrain of Cyber*. Georgetown Journal of International Affairs, International Engagement on Cyber, 2012, 99

[12] Fanelli R. and Conti G., "*A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict*," in 4th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, June 2012.

[13] Raymond, David et al, 7

[14] Raymond, David, G. Conti, T. Cross and R. Fanelli, "*A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons*," in 5th International Conference on Cyber Conflict, Tallinn, Estonia, June 2013.

[15] Raymond, David et al, 7

[16] Kern, Lt Colonel Sean Charles Gaines, *Expanding Combat Power Through Military Cyber Power Theory*. Joint Force Quarterly (JFQ), Issue 79, 4th Quarter, National Defense University Press, October 2015, 89

[17] Ibid.

[18] Williams, Brett T. "*Cyberspace: What is it, where is it and who cares?*," Armed Forces Journal (March 13, 2014)

[19] Ibid.

[20] U.S. Department of Defense, *The DoD Cyber Strategy,* April, 2015, 7

[21] Lanham, Lt Colonel Michael, *Cyber defense planning, Operating on Unconventional Terrain*. U.S. Army Signal Center of Excellence, Army Communicator, Signal Towers (Building 29808), Room 713, Fort Gordon, GA, 0905-5301, 2012, 9

[22] Bodeau, Deborah et al, *Mapping the Cyber Terrain*. MITRE Technical Report MTR10433, The MITRE Corporation, November 2013, 1

[23] Ibid.

[24] Ibid, 2

[25] Ibid, 2

[26] Ibid.

[27] Ibid.,5

[28] Mills, John R., 100

[29] Holsopple, Jared, et. al, *"FuSIA: Future Situation and Impact Awareness"*, Inf. Exploitation Group, CUBRC, Buffalo, NY, 11th International Conference on Information Fusion, 2008, Figure 4

[30] Fava, D., et. al., "Terrain and behavior modeling for projecting multistage cyber attacks," in *Proceedings of the 10th International Conference on Information Fusion*, Quebec, 2007, 1

[31] Jakobson, G., *"Extending Situation Modeling with Inference of Plausible Future Cyber 35 Situations,"* in 2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision *Support (CogSIMA)*, Miami Beach, FL, 9 July 2007, 1

[32] Ibid.

[33] U.S. Department of Defense, Joint Publication 3-12 (R), *Cyberspace Operations*, 5 February 2013, II 8

[34] The DoD Cyber Strategy, 6

[35] Cyberspace Operations, , III 6

[36] Raymond, David et al, 1

[37] U.S. Air Force, ANNEX 3-12

[38] Joint Publication 3-12 (R)

[39] Ibid, I-V

[40] Raymond, David et al, 7

[41] Bodeau, Deborah et al, 1

[42] Ibid, III 6

[43] *The DoD Cyber Strategy*

[44] Curtis E. Lemay Center, Annex 3-30 Command and Control, Appendix B: The Air Operations Center

[45] U.S. Department of Defense, Joint Publication 3-30, Command and Control of Joint Air Operations. 10 February 2014, E1

[46] Air Force Instruction 13-1AOC, Volume 3, *Operational Procedures-Air Operations Center (Aoc),*38

[47] Joint Publication 3-12 (R), I-2

[48] The DoD Cyber Strategy, 19-21

[49] Raymond, David et al, 1

[50] Revised from U.S. Department of Defense, Joint Publication 5-0, *Joint Operation Planning,* Figure IV-14, IV38

Bibliography

Air Force Instruction 13-1AOC, Volume 3, Operational Procedures-Air Operations Center (AOC)

Bodeau, Deborah et al, Mapping the Cyber Terrain. MITRE Technical Report MTR10433, The MITRE Corporation, November 2013.

Curtis E. Lemay Center, Annex 3-30 Command and Control, Appendix B: The Air Operations Center

Fanelli R. and Conti G., "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict," in 4th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, June 2012.]

Fava, D., et. al., and Argauer B., "Terrain and behavior modeling for projecting multistage cyber attacks," in Proceedings of the 10th International Conference on Information Fusion, Quebec, 2007

Gilmore, J. Michael, Information Assurance (IA) and Interoperability (IOP). DOT&E FY2012 Annual Report, December, 2012.

Headquarters, Department of the Army, Field Manual 3-90-1: Offense and Defense Volume 1, 2013

Holsopple, Jared, et. al, "FuSIA: Future Situation and Impact Awareness", Inf. Exploitation Group, CUBRC, Buffalo, NY, 11th International Conference on Information Fusion, 2008, Figure 4

Jakobson G., "Extending Situation Modeling with Inference of Plausible Future Cyber 35 Situations," in 2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), Miami Beach, FL, 9 July 2007

Kern, Lt Colonel Sean Charles Gaines, Expanding Combat Power Through Military Cyber Power Theory. Joint Force Quarterly (JFQ), Issue 79, 4th Quarter, National Defense University Press, October 2015.

Lanham, Lt Colonel Michael, Cyber defense planning, Operating on Unconventional Terrain. U.S. Army Signal Center of Excellence, Army Communicator, Signal Towers (Building 29808), Room 713, Fort Gordon, GA, 0905-5301, 2012.

Libicki, Martin C, Cyberspace Is Not a Warfighting Domain. I/S: A Journal of Law and Policy, Vol. 8:2, 2012.

Mills, John R., The Key Terrain of Cyber. Georgetown Journal of International Affairs, International Engagement on Cyber, 2012.

Raymond, David et al, Key Terrain in Cyberspace: Seeking the High Ground. 2014 6th International Conference on Cyber Conflict, NATO CCD COE Publications.

Raymond, David, G. Conti, T. Cross and R. Fanelli, "A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons," in 5th International Conference on Cyber Conflict, Tallinn, Estonia, June 2013

U.S. Air Force, ANNEX 3-12 Cyberspace Operations. 30 November 2011.

U.S. Department of Defense, The DoD Cyber Strategy, April, 2015

U.S. Department of Defense, Joint Publication 2-01.3 Joint Intelligence Preparation of the Operational Environment, 16 June 2009, xi

U.S. Department of Defense, Joint Publication 3-12 (R), Cyberspace Operations, 5 February 2013, III 6

U.S. Department of Defense, Joint Publication 3-30, Command and Control of Joint Air Operations. 10 February 2014.

Williams, Brett T. "Cyberspace: What is it, where is it and who cares?," Armed Forces Journal (March 13, 2014)

Williams, Brett T. "Ten Propositions Regarding Cyberspace Operations," Joint Force Quarterly 61 (2nd Quarter 2011)

Williams, Major General Brett T., The Joint Force Commander's Guide to Cyberspace Operations. Joint Force Quarterly (JFQ), Issue 73, 2th Quarter, National Defense University Press, April 2014.ibicki, Martin C. 2012. "Cyberspace is Not a Warfighting Domain." *I/S: A Journal of Law and Policy* 8:2: 12-13.